

Security Supplement  
to the  
Software Communications Architecture Specification

**APPENDIX A**

**Functional Security Requirements for JTRS**

Revision Summary

1.0	Initial Release
-----	-----------------

## Requirements Matrix for JTRS Security Functions

		Gross Category														
		Encrypt	Decrypt	Control	Status	I&A	Keystream (TRANSEC)	Bypass	Algo Mgmt	Key Mgmt	Time	Algo Control	Correlate	Key ID	NA	
01	Alarm Crypto														x	RTOS interrupts for shutdowns - maintain channel availability
02	Alarm Indicate				x											Pass indicator to HMI - Alarm ALL and "selective"
03	Encrypt Red Side	x														Standard user data, authenticate
04	Decrypt Red Side		x													Standard user data, authenticate
05	Encrypt Black Side	x														Orderwire (e.g., DAMA)
06	Decrypt Black Side		x													Orderwire (e.g., DAMA)
07	Crypto TRANSEC Stream						x									Standard
08	Modem TRANSEC Stream														x	Modem implementation of TRANSEC generation
09	External Use of TRANSEC Keys									x						Pass keys from KG to modem
10	Use TRANSEC Bits														x	Low latency - freq, clock, shape effects
11	Use Time Of Day (TOD)										x					Specific to KG synchronization
12	Sense Patterns												x			Related to received headers
13	Sync/Resync											x				Internal to KG function - report status
14	Store RED Data														x	
15	Store BLACK Data			x												
16	View INFOSEC Resources			x	x											Need access from KG function
17	Zeroize (All & Selective)			x	x					x						Internal with hard switch?
18	Erase Algorithm			x	x				x							Refers to a BLACK image of cryptographic algorithm - non-Modem
19	Create Channel(Program Crypto)			x	x				x							Install the crypto parameters
20	Load External Algorithm			x		x			x							This function can stay BLACK
21	Instantiate Algorithm								x							Internal decrypt and usage
22	Select Algorithm Mode			x												Waveform has to provide KG mode settings
23	Load Black Key			x	x					x						Assume DS-101 - can be non-fill port
24	Load Red Key			x	x					x				x		DS-102 or DS-101
25	Develop Key			x			x			x						Use in internal authentication, storage, and pair-wise processes

## Requirements Matrix for JTRS Security Functions

Gross Category														
	Encrypt	Decrypt	Control	Status	I&A	Keystream (TRANSEC)	Bypass	Algo Mgmt	Key Mgmt	Time	Algo Control	Correlate	Key ID	NA
26 Store Key RED														x Volatile storage only - overwrite erasure required
27 Store key BLACK														x Use of internal algorithm and form of KEK
28 Select & Use Key			x						x				x	Binding of keys and IDs/Tags - auto rollover option?
29 Initialize KG														x Randomizer function
30 Zeroize External			x											Total zeroization - front panel
31 Zeroize Automatic (TOD)			x	x						x				Provide an HMI prompt for the action
32 Rekey Over The Air	xt	x	xt	x										Sense patterns - wrap/unwrap
33 Zeroize Over The Air	xt	x	xt		x									Sense patterns - authenticate
34 Transfer Key Over the Air			x											Sense patterns - decrypt, store
35 Update Key			x						x				x	Internal to KG
36 Support External Crypto														x Black I/O or BLACK channel created
37 Support Control Bypass			x		x		xrun							Monitor - primarily RED to BLACK
38 Support User Data Bypass (PT)														x Monitor - RED to BLACK
39 Support Protocol Bypass			x		x		xrun							Monitor - RED to BLACK
40 Support Header Bypass			x		x		xrun							Monitor - RED to BLACK
41 Simultaneous Multi-Channel Ops														1 Channel separation and coexistence
42 Support Crossbanding														x Can be RED or BLACK - privilege comparison and data flow
43 Support Digital Signatures					x									Cryptographic function - can be RED-RED
44 Support Authentication					x									User - Can be cryptographic depending on level of assurance
45 Load Access Control Table			x											Protected storage
46 Support non-Repudiation					x									Does this involve a third party?
47 Support System Declassification(CIK)			x											This is a box level function.
48 Support Channel Declassification														x RED memory clearing required at channel reconfiguration
49 Establish Privileges					x									Refers to access - Admin/ User - distinguish role types - up to 64

## Requirements Matrix for JTRS Security Functions

Gross Category														
	Encrypt	Decrypt	Control	Status	I&A	Keystream (TRANSEC)	Bypass	Algo Mgmt	Key Mgmt	Time	Algo Control	Correlate	Key ID	NA
50 Control Access					x									Decision point and execution required - enforce privileges
51 Build Wireless Access Controls					x									Protected storage
52 Build Wired User Access Controls					x									Redundant?
53 Run Access Control					x									Redundant?
54 Build ID/Authentication Functions					x									Protected storage
55 Identify and Authenticate Users					x									Decision point and execution required
56 Identify Security Resources			x	x										Need to collect all parameters for HMI/Ext I/F
57 Authenticate Software Downloads					x									Signatures and integrity checks
58 Verify Software Files (Internal)					x									Perform integrity checks - (e.g., CRC or Hash)
59 Monitor & Alarm Information Paths			x	x									2	A guard or process monitor function
60 (Get) Establish Security Policy			x											How about "Aggregate Security Policies"?
61 Enforce Security Policy/Status													x	KG alarms and lower level alerts
62 Monitor Channels													x	Redundant to 59
63 Cover External Network Addresses													x	For transmitted data
64 Protect Internal Network Address													x	Protected addr space - network mgr SAC - isolate int and ext
65 Audit/Report Security Events			x											Protected storage - collect and store data
66 Detect/Report Intrusion (Internet)													3	Protected storage - applies for both wired and wireless access
67 Detect/Report Viruses													3	Protected storage - applies for both wired and wireless access
68 Detect/Act On Tampering				x										Policy determines actions taken - hardware required
69 Monitor/Respond to Alarms/Events													x	Enforce alarm/event policy

## Requirements Matrix for JTRS Security Functions

Gross Category		Encrypt	Decrypt	Control	Status	I&A	Keystream (TRANSEC)	Bypass	Algo Mgmt	Key Mgmt	Time	Algo Control	Correlate	Key ID	NA	
70	Support Security Related HMI Funcs			x												Refers to items such as COMSEC mode and key select
71	Support Data Separation														x	
72	Support Process Separation														x	
73	Support Classified Applications														x	If program parameters are modified, symmetric crypto required
75	Support Algorithm Storage			x												BLACK storage
75	Maintain Internal Data Integrity														4	Long term storage/retrieval - and during real time transport
76	Maintain User Data Integrity														4	Are internal integrity checks required? - Good radio practice
77	Support Memory Separation														x	Redundant with 71
78	Establish Information Paths			x												Internal crypto module paths are independent of FCA and RTOS
79	Maintain Information Path Validity														x	
80	Set Policy for Storing Information														5	Subset to 60
81	Set Policy for Controlling Access														5	Subset to 60
82	Set Policy for Separating Data														5	Subset to 60
83	Set Policy for Separating Processes														5	Subset to 60
84	Set Policy for Alarm Response														5	Subset to 60
85	Manage Keys and Algorithms			x					x	x						Move up with KM subset items
86	Boot to Known State				x											Radio responsibility
87	Monitor Boot Status			x												Must invoke warnings and alarms
88	Secure Recovery of Operation														x	Must return to known secure state - operating
89	Failure to Known Safe State				x											Must return to known secure state - no operation

## Requirements Matrix for JTRS Security Functions

Gross Category		Encrypt	Decrypt	Control	Status	I&A	Keystream (TRANSEC)	Bypass	Algo Mgmt	Key Mgmt	Time	Algo Control	Correlate	Key ID	NA	
90	TEMPEST														x	Operations (e.g., keying) must continue during RF operation (wet)
91	Separate RED /BLACK Electrical														x	Part of TEMPEST function
92	Power Transient Detect (PTD)				x											PTD targeted to KG alarm and reset - need RED memory erase
93	Accept KG Identification				x											
94	Secure Recovery of Operation - Channel			x												
95	Recognize Algorithm Versions				x											
96	Tear Down Channel			x												

### Notes

- 1 Load Key behavior must validate same classification levels is used for all channels used in system high config
- 2 Need to add to system API
- 3 HMI type Guard and API for reporting
- 4 Must Perform CRC Checks and Generation and checks prior to SW usage
- 5 Radio Level Policy Profile to be Loaded as a SAC, Prior to channel setup, Compare classification of key with instantiation to enforce separation

